VistA System Monitor (VSM) 3.0

Deployment, Installation, Back-Out, and Rollback Guide (DIBRG) (REDACTED)

July 2020

Department of Veterans Affairs (VA)

Office of Information and Technology (OIT)

Enterprise Program Management Office (EPMO)

Capacity and Performance Engineering (CPE)

Revision History

Date	Revision	Description	Author

07/22/2020	1.0	Initial VistA System Monitor (VSM) 3.0 Deployment, Installation, Back-Out, and Rollback Guide (DIBRG):
		• Converted the current Installation Guide into a Deployment, Installation, Back-Out, and Rollback Guide (DIBRG) via the DIBRG template Version 2.2, released on March 2016.
		• Upgraded to real time VistA System Monitor 3.0.
		• Changed transmission to real time using HyperText Transport Protocol (HTTP).
		• Updated the following monitors:
		  ○ VistA Timed Collection Monitor (VTCM)
		  ○ VistA Storage Monitor (VSTM)
		  ○ VistA Business Event Monitor (VBEM)
		  ○ VistA Message Count Monitor (VMCM)
		  ○ VistA HL7 Monitor (VHLM)
		• Added the following new monitors:
		  ○ Vista Coversheet Monitor (VCSM).
		  ○ VistA Error Trap Monitor (VETM).
			Enterprise Program Management Office (EPMO) Capacity and Performance Engineering (CPE)

Table of Contents

List of Figures

List of Tables

Orientation

How to Use this Manual

The Deployment, Installation, Back-out, and Rollback Guide (DIBRG) defines the ordered, technical steps required to install the product, and if necessary, to back out the installation, and roll back to the previously installed version of the product.

Throughout this manual, advice and instructions are offered regarding the use of VistA System Monitor (VSM) 3.0 software and the functionality it provides for Veterans Health Information Systems and Technology Architecture (VistA) software products.

Intended Audience

The intended audience of this manual is the following stakeholders:

- **Enterprise Program Management Office (EPMO)—**System engineers and Capacity Management personnel responsible for enterprise capacity planning and system architecture.
- **System Administrators—**System administrators and Capacity Management personnel at local and regional Department of Veterans Affairs (VA) sites who are responsible for computer management and system security on the VistA M Servers.
- **EPMO Developers—**VistA legacy development teams.
- **Product Support (PS)**.

Disclaimers

Software Disclaimer

This software was developed at the Department of Veterans Affairs (VA) by employees of the Federal Government in the course of their official duties. Pursuant to title 17 Section 105 of the United States Code this software is *not* subject to copyright protection and is in the public domain. VA assumes no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic. We would appreciate acknowledgement if the software is used. This software can be redistributed and/or modified freely provided that any derivative works bear some notice that they are derived from it, and any modified versions bear some notice that they have been modified.

Documentation Disclaimer

This manual provides an overall explanation of using the VistA System Monitor (VSM) 3.0 software; however, no attempt is made to explain how the overall VistA programming system is integrated and maintained. Such methods and procedures are documented elsewhere. We suggest you look at the various VA Internet and Intranet SharePoint sites and websites for a general orientation to VistA. For example, visit the Office of Information and Technology (OIT) Enterprise Program Management Office (EPMO) Intranet Website.

DISCLAIMER: The appearance of any external hyperlink references in this manual does *not* constitute endorsement by the Department of Veterans Affairs (VA) of this Website or the information, products, or services contained therein. The VA does *not* exercise any editorial control over the information you find at these locations. Such links are provided and are consistent with the stated purpose of this VA Intranet Service.

Documentation Conventions

This manual uses several methods to highlight different aspects of the material:

- Various symbols are used throughout the documentation to alert the reader to special information. Table 1 gives a description of each of these symbols:

Table 1: Documentation Symbol Descriptions

Symbol	Description
	**NOTE / REF:** Used to inform the reader of general information including references to additional reading material.
	**CAUTION / RECOMMENDATION / DISCLAIMER:** Used to caution the reader to take special notice of critical information.
	**SPECIAL INSTALLATION NOTE:** Used to denote special installation instructions only (e.g., virgin installations or platform-specific steps).

- Descriptive text is presented in a proportional font (as represented by this font).
- Conventions for displaying TEST data in this document are as follows:
  - The first three digits (prefix) of any Social Security Numbers (SSN) begin with either "**000**" or "**666**".
  - Patient and user names are formatted as follows:
    - <*APPLICATION NAME/ABBREVIATION/NAMESPACE*>PATIENT,<*N*>
    - <*APPLICATION NAME/ABBREVIATION/NAMESPACE*>USER,<*N*>

    Where "<*APPLICATION NAME/ABBREVIATION/NAMESPACE*>" is defined in the Approved Application Abbreviations document and "<*N*>" represents the first name as a number spelled out or as a number value and incremented with each new entry.

For example, in VSM (**KMP**) test patient and user names would be documented as follows:

- KMPPATIENT,ONE or KMPUSER,ONE
- KMPPATIENT,TWO or KMPUSER,TWO
- KMPPATIENT,THREE or KMPUSER,THREE
- KMPPATIENT,14 or KMPUSER,14
- Etc.

- "Snapshots" of computer online displays (i.e., screen captures/dialogues) and computer source code is shown in a *non*-proportional font and may be enclosed within a box.
  - User's responses to online prompts are **bold** typeface and highlighted in yellow (e.g., **<Enter>**). The following example is a screen capture of computer dialogue, and indicates that the user should enter two question marks:

```
Select Primary Menu option: ??
```

  - Emphasis within a dialogue box is **bold** typeface and highlighted in blue (e.g., STANDARD LISTENER: RUNNING).
  - Some software code reserved/key words are **bold** typeface with alternate color font.
  - References to "**<Enter>**" within these snapshots indicate that the user should press the **Enter** key on the keyboard. Other special keys are represented within < > angle brackets. For example, pressing the **PF1** key can be represented as pressing **<PF1>**.
  - Author's comments are displayed in italics or as "callout" boxes.

NOTE: Callout boxes refer to labels or descriptions usually enclosed within a box, which point to specific areas of a displayed image.

- This manual refers to the M programming language. Under the 1995 American National Standards Institute (ANSI) standard, M is the primary name of the MUMPS programming language, and MUMPS is considered an alternate name. This manual uses the name M.
- All uppercase is reserved for the representation of M code, variable names, or the formal name of options, field/file names, and security keys (e.g., the XUPROGMODE security key).

NOTE: Other software code (e.g., Delphi/Pascal and Java) variable names and file/folder names can be written in lower or mixed case (e.g., CamelCase).

Documentation Navigation

This document uses Microsoft® Word's built-in navigation for internal hyperlinks. To add **Back** and **Forward** navigation buttons to the toolbar, do the following:

1. Right-click anywhere on the customizable Toolbar in Word (*not* the Ribbon section).
2. Select **Customize Quick Access Toolbar** from the secondary menu.
3. Select the drop-down arrow in the "**Choose commands from:**" box.
4. Select **All Commands** from the displayed list.
5. Scroll through the command list in the left column until you see the **Back** command (circle with arrow pointing left).
6. Select/Highlight the **Back** command and select **Add** to add it to your customized toolbar.
7. Scroll through the command list in the left column until you see the **Forward** command (circle with arrow pointing right).
8. Select/Highlight the **Forward** command and select **Add** to add it to the customized toolbar.
9. Select **OK**.

You can now use these **Back** and **Forward** command buttons in the Toolbar to navigate back and forth in the Word document when selecting hyperlinks within the document.

NOTE: This is a one-time setup and is automatically available in any other Word document once you install it on the Toolbar.

How to Obtain Technical Information Online

Exported VistA M Server-based software file, routine, and global documentation can be generated using Kernel, MailMan, and VA FileMan utilities.

NOTE: Methods of obtaining specific technical information online is indicated where applicable under the appropriate section.

REF: For further information, see the *VistA System Monitor (VSM) Technical Manual*.

Help at Prompts

VistA M Server-based software provides online help and commonly used system default prompts. Users are encouraged to enter question marks at any response prompt. At the end of the

help display, you are immediately returned to the point from which you started. This is an easy way to learn about any aspect of VistA M Server-based software.

Obtaining Data Dictionary Listings

Technical information about VistA M Server-based files and the fields in files is stored in data dictionaries (DD). You can use the **List File Attributes** [DILIST] option on the **Data Dictionary Utilities** [DI DDU] menu in VA FileMan to print formatted data dictionaries.

REF: For details about obtaining data dictionaries and about the formats available, see the "List File Attributes" section in the "File Management" section in the *VA FileMan Advanced User Manual*.

Assumptions

This manual is written with the assumption that the reader is familiar with the following:

- VistA computing environment:
  - Kernel—VistA M Server software
  - VA FileMan data structures and terminology—VistA M Server software
- Microsoft® Windows environment
- M programming language

Reference Materials

Readers who wish to learn more about VSM should consult the following:

- *VistA System Monitor (VSM) Deployment, Installation, Back-Out, and Rollback Guide (DIBRG)* (this manual)
- *VistA System Monitor (VSM) User Manual*
- *VistA System Monitor (VSM) Technical Manual*

VistA documentation is made available online in Microsoft® Word format and in Adobe® Acrobat Portable Document Format (PDF). The PDF documents *must* be read using the Adobe® Acrobat Reader, which is freely distributed by Adobe® Systems Incorporated at: http://www.adobe.com/

VistA documentation can be downloaded from the VA Software Document Library (VDL): http://www.va.gov/vdl/

REF: See the VistA System Monitor (VSM) manuals on the VDL.

VistA documentation and software can also be downloaded from the Product Support (PS) Anonymous Directories.

1 Introduction

The Veterans Health Information Systems and Technology Architecture (VistA) System Monitor (VSM) 3.0 software collects Caché and VistA metrics related to system capacity and business usage. The package is made up of multiple collectors. The KMP*4.0*1 patch upgraded the following five collectors to provide data in real time:

- **VistA Timed Collection Monitor (VTCM)—**Collects Caché metrics at regularly scheduled intervals such that they can be used in conjunction with metrics gathered via other deployed collection tools.
- **VistA Storage Monitor (VSTM)—**Collects storage metrics for each database once daily.
- **VistA Business Event Monitor (VBEM)—**Collects Cache metrics for VistA functions (Menu Options, TaskMan Jobs and Remote Procedure Calls).
- **VistA Message Count Monitor (VMCM)—**Collects inbound and outbound Health Level Seven (HL7) and HL7 Optimized (HLO) message counts at regularly scheduled intervals.
- **VistA HL7 Monitor (VHLM)—**Collects metadata about HL7 messages (**SYNC** and **ASYNC**) as well as HLO messages.

Additionally, the KMP*4.0*1 patch deployed the following two monitors:

- **Vista Coversheet Monitor (VCSM)—**Collects timing metrics related to the Computerized Patient Record System (CPRS) coversheets.
- **VistA Error Trap Monitor (VETM)—**Collects data from the sites Kernel Error Trap, ERROR LOG (#3.075) file.

This data is used for understanding VistA systems as they relate to the infrastructure on which they are deployed and to provide data for application performance monitoring.

1.1 Purpose

The purpose of this guide is to provide instructions for deploying and installing the VistA Capacity and Performance Engineering (CPE) VistA System Monitor (VSM) 3.0 software (KMP*4.0*1 patch).

1.2 Dependencies

This section lists and describes all application, system, financial, and other dependencies for this deployment, including upstream processing.

There are no dependencies for VSM 3.0 Patch KMP*4.0*1 release other than the operating system and software dependencies described in Section 3.3.2, "Software."

1.3 Constraints

There are no constraints for VSM 3.0 Patch KMP*4.0*1 release other than the operating system and software dependencies described in Section 3.3.2, "Software."

2 Roles and Responsibilities

This section lists the teams that will perform the steps described in this guide.

Table 2 identifies the technical and support personnel who are involved in the deployment, installation, back-out, and rollback of the Veterans Health Information Systems and Technology Architecture (VistA) System Monitor (VSM) 3.0 software (KMP*4.0*1) release.

Table 2: Deployment, Installation, Back-Out, and Rollback Roles and Responsibilities

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
1	Enterprise Program Management Office (EPMO) Implementation Team	Deployment	Plan and schedule deployment (including orchestration with vendors).	Planning
2	EPMO Implementation Team	Deployment	Determine and document the roles and responsibilities of those involved in the deployment.	Planning
3	Software Quality Assurance (SQA)	Deployment	Test for operational readiness.	Build
4	Product Support (PS)	Deployment	Execute deployment.	Release Prep Phase
5	EPMO Implementation Team	Installation	Plan and schedule installation.	Build Phase
6	EPMO Implementation Team Capacity and Performance Engineering (CPE) Team	Back-Out	Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out).	Build Phase
7	SDE Field Operations (FO) Enterprise Operations (EO)	Post Deployment	Hardware, Software and System Support.	Post Release

3 Deployment

This section provides the schedule and milestones for the VSM 3.0 Patch KMP*4.0*1 deployment.

The VSM 3.0 Patch KMP*4.0*1 deployment is planned as a simultaneous rollout. National release is scheduled for **August 2020**.

3.1 Timeline

The VSM 3.0 Patch KMP*4.0*1 deployment and installation is scheduled to run for **30** days from release, which is the typical Veterans Health Information Systems and Technology Architecture (VistA) national patch rollout schedule.

Table 3 provides an *estimate* of the VSM 3.0 Patch KMP*4.0*1 deployment timeline dates:

Table 3: VSM 3.0 Patch KMP*4.0*1 Deployment Timeline

Deployment	Start	Finish
Patch Development and Release	**1/1/2020**	**8/1/2020**
Site Installation and Deployment	**8/1/2020**	**8/31/2020**
Sustainment	**9/1/2020**	**N/A**

3.2 Site Readiness Assessment

This section describes the Site Readiness Assessment for the locations that will receive the VSM 3.0 Patch KMP*4.0*1 deployment. This will be a typical national release of a VistA patch to all VistA production sites.

Topology determinations are made by Enterprise Systems Engineering (ESE) and vetted by Field Office (FO), National Data Center Program (NDCP), and Austin Information Technology Center (AITC) during the design phase as appropriate. Field site coordination is done by FO unless otherwise stipulated by FO.

3.2.1 Deployment Topology (Targeted Architecture)

This section describes the deployment topology (local sites, etc.) for VSM 3.0 Patch KMP*4.0*1.

VSM 3.0 Patch KMP*4.0*1 will be distributed to local and regional system administrators and support personnel responsible for each of the **130** VistA parent systems. The actual code will be available to developers from the Product Support (PS) Anonymous Directories. (The code will be available to developers from secure file transfer (SFTP) sites listed in the patch description.)

3.2.2 Site Information (Locations, Deployment Recipients)

This section describes the physical locations (sites) that will host the deployed VSM 3.0 Patch KMP*4.0*1.

The VSM 3.0 Patch KMP*4.0*1 code is directly deployed to VA sites.

3.2.3 Site Preparation

This section describes the preparation required for the site at which the system will operate.

There are no special site preparations or changes that *must* occur to the operational site and no specific features or items that need to be modified to adapt to VSM 3.0 Patch KMP*4.0*1.

As a precursor to the VSM 3.0 Patch KMP*4.0*1 deployment, the VSM documentation set (including this *Deployment, Installation, Back-Out, and Rollback Guide [DIBRG]*) will be added to the VA Software Document Library (VDL) at:
https://www.va.gov/vdl/application.asp?appid=218

Table 4 describes preparation required by the site prior to deployment.

Table 4: Site Preparation

Site/Other	Problem/Change Needed	Features to Adapt/Modify to New Product	Actions/Steps	Owner
Not Applicable (N/A)	N/A	N/A	N/A	N/A

3.3 Resources

This section describes the hardware, software, facilities, documentation, and any other resources, other than personnel, required for the VSM 3.0 Patch KMP*4.0*1 deployment and installation.

3.3.1 Hardware

There are no specific hardware requirements for installation of VSM 3.0 Patch KMP*4.0*1. There is also no need for specific hardware to assist in the deployment of VSM 3.0 Patch KMP*4.0*1.

Table 5 describes hardware specifications required at each site prior to deployment.

Table 5: Hardware Specifications

Required Hardware	Model	Version	Configuration	Manufacturer	Other
Not Applicable (N/A)	N/A	N/A	N/A	N/A	N/A

REF: For details about who is responsible for preparing the site to meet these hardware specifications, see Table 2.

3.3.2 Software

The following minimum software tools are required on your VistA Server in order to install and use the VSM 3.0 Patch KMP*4.0*1 software:

- VistA System Monitor 2.0 *must* already be installed. This includes patch releases: XU*8.0*568 and XU*8.0*670.
- VistA account running on InterSystems' Caché for Linux, NT, or OpenVMS.
- VistA accounts *must* contain the fully patched versions of the following packages:
  - Kernel 8.0
  - Kernel Toolkit 7.3
  - MailMan 8.0
  - VA FileMan 22.2
  - VSM 2.0

REF: For details about who is responsible for preparing the site to meet these software specifications, see Table 2.

3.3.3 Communications

This section describes any notifications activities and how they will occur.

Prior to the deployment of the VSM 3.0 Patch KMP*4.0*1 release, a product announcement will be sent via email to current Points of Contact (POC) on record for each site describing the product and a brief description of the deployment and post-deployment support. Included will be links to the VSM 3.0 VA Software Document Library (VDL) and Rational/GitHub repositories, which contain further information about the release and the deployment, including the deployment schedule and required pre-installation activities.

The VSM 3.0 Patch KMP*4.0*1 Implementation Team will respond to email requests for assistance and further information and, where appropriate, re-direct these requests to specialist technical staff.

3.3.3.1 Deployment/Installation/Back-Out Checklist

Tracking of installation for VSM 3.0 Patch KMP*4.0*1 is monitored in FORUM.

Table 6 provides a checklist to be used to capture the coordination effort and document the day/time/individual when each activity (deploy, install, back-out) is completed for VSM 3.0 patch releases.

Table 6: Deployment/Installation/Back-Out Checklist

Activity	Day	Time	Individual who completed task
Deploy			
Install			
Back-Out			

4 Installation

4.1 Pre-Installation and System Requirements

The following minimum software tools are required on your VistA Server in order to install and use the VSM 3.0 Patch KMP*4.0*1 software:

- VistA System Monitor (VSM) 2.0 *must* already be installed. This includes patch releases: XU*8.0*568 and XU*8.0*670.
- VistA account running on InterSystems' Caché for Linux, NT, or OpenVMS.
- VistA accounts *must* contain the fully patched versions of the following packages:
  - Kernel 8.0
  - Kernel Toolkit 7.3
  - MailMan 8.0
  - VA FileMan 22.2*
  - VSM 1.0

NOTE: These software packages *must* be properly installed and fully patched *prior* to installing the VSM 3.0 Patch KMP*4.0*1 software distribution. Patches *must* be installed in published sequence. You can obtain all released VistA patches (including patch description and installation instructions), from the National Patch Module (NPM) on FORUM or through normal procedures.

4.2 Platform Installation and Preparation

It is *recommended* that sites take the following approach to installing the VistA System Monitor (VSM) 3.0 software:

1. Obtain the VSM 3.0 documentation.
2. Install the software into a Test account.
3. Install the software into a Production system.

The installation of VistA System Monitor (VSM) 3.0 software only affects the VSM options. Therefore, this installation can be performed at any time of the day with no disruption. Installation should take approximately **2** minutes.

4.3 Download and Extract Files

4.3.1 Software

The initial deployment of the VistA System Monitor (VSM) 3.0 software is released via the National Patch Module (NPM) on FORUM using MailMan and Kernel Installation & Distribution System (KIDS); there is no host file with this patch. Use KIDS to install the VistA System Monitor (VSM) 3.0 software.

The purpose of VSM 3.0 is to upgrade the following as part of the Capacity Management (**KMP***) VistA System Monitor (**KMP**) tools suite to real time metric transmission:

- **VistA Timed Collection Monitor (VTCM)—**Collects Caché metrics at regularly scheduled intervals such that they can be used in conjunction with metrics gathered via other deployed collection tools.
- **VistA Storage Monitor (VSTM)—**Collects storage metrics for each database once daily.
- **VistA Business Event Monitor (VBEM)—**Collects Cache metrics for VistA functions (Menu Options, TaskMan Jobs and Remote Procedure Calls).
- **VistA Message Count Monitor (VMCM)—**Collects inbound and outbound Health Level Seven (HL7) and HL7 Optimized (HLO) message counts at regularly scheduled intervals.
- **VistA HL7 Monitor (VHLM)—**Collects metadata about HL7 messages (**SYNC** and **ASYNC**) as well as HLO messages.

Additionally, the following two monitors will be deployed:

- **Vista Coversheet Monitor (VCSM)—**Collects timing metrics related to the CPRS coversheets.
- **VistA Error Trap Monitor (VETM)—**Collects data from the sites Kernel Error Trap, ERROR LOG (#3.075) file.

4.3.2 Documentation

Documentation for Vista System Monitor (VSM) is available on the VA Software Document Library (VDL) at: http://www.va.gov/vdl/application.asp?appid=218.

VistA documentation and software can also be downloaded from the Product Support (PS) Anonymous Directories via Secure File Transfer Protocol (SFTP).

Table 7: VSM Documentation

File Name	FTP Mode	Description
kmp_dibrg.pdf	Binary	VSM Deployment, Installation, Back-out, and Rollback Guide
kmp_um.pdf	Binary	VSM User Manual
kmp_tm.pdf	Binary	VSM Technical Manual

4.4 Database Creation

The VSM 3.0 software installation does *not* create any databases. VSM uses the existing VA FileMan database.

4.5 Installation Scripts

There are no installation scripts for the Vista System Monitor (VSM) 3.0 software installation.

4.6 Cron Scripts

There are no cron scripts for the Vista System Monitor (VSM) 3.0 software installation.

4.7 Access Requirements and Skills Needed for the Installation

The installer needs to know how to do the following:

- Obtain VistA software from FORUM.
- Run a Kernel Installation and Distribution System (KIDS) installation.
- Use the VistA **Systems Manager Menu** [EVE]EVE menu.

4.8 Installation Procedure

4.8.1 Patch Installation Instructions

Patch installation instructions are documented in VSM 3.0 Patch KMP*4.0*1 on FORUM. This is a standard VistA patch installation. Use the Kernel Installation & Distribution System (KIDS) to install the VistA System Monitor (VSM) 3.0 software. Monitors will be started automatically on production systems.

This installation updates the following VSM files in the **^KMPV** global:

- **VSM CONFIGURATION (#8969):** Contains configuration parameters for each monitor and most recent run times.
- **VSM MONITOR DEFAULTS (#8969.02):** Contains default configuration parameters for each monitor allowing restoration of monitor defaults.
- **VSM CACHE TASK LOG (#8969.03):** Contains run time for each monitor and node for forensic purposes. This file will be purged upon each monitor run to contain a maximum of **six** (**6**) months of entries.

The **^KMPTMP("KMPV")** global is used to store temporary VSM data. To ensure global size is kept to a minimum, a purge function is run at the daily start of all monitors. Data is kept only up to the maximum number of days configured in the VSM CONFIGURATION (#8969) file. This parameter has a maximum of **seven** (**7**) days.

CAUTION: The ^KMPTMP("KMPV") global should *not* be journaled!

REF: Details regarding imported files, options, protocols, etc. can be found in the *VSM Technical Manual*.

4.8.2 Caché Task Manager

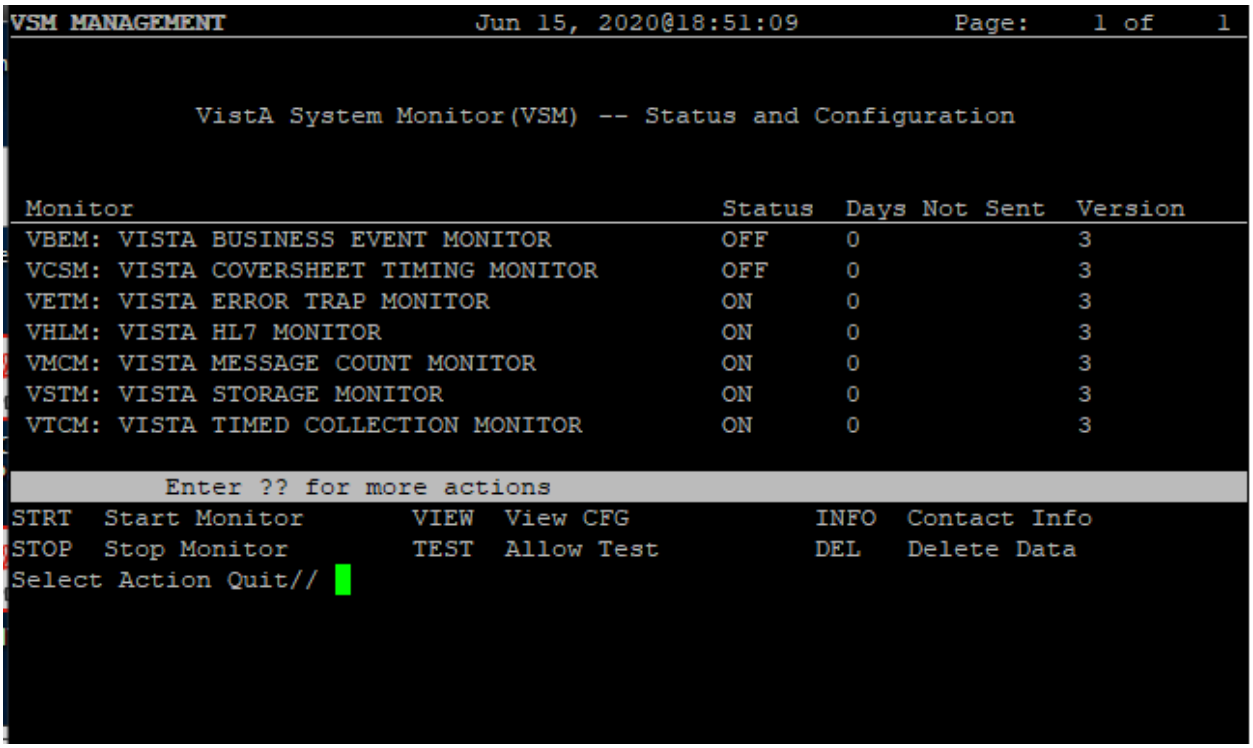
The VistA System Monitors are dependent on the Caché Task Manager to start the collection routine each morning on each node of the VistA environment.

4.9 Installation Verification Procedure

To verify the VSM installation, do the following:

1. Use the **VSM MANAGEMENT** [KMPV VSM MANAGEMENT] option located under the **Capacity Planning** [XTCM MAIN] option to verify the VSM installation:

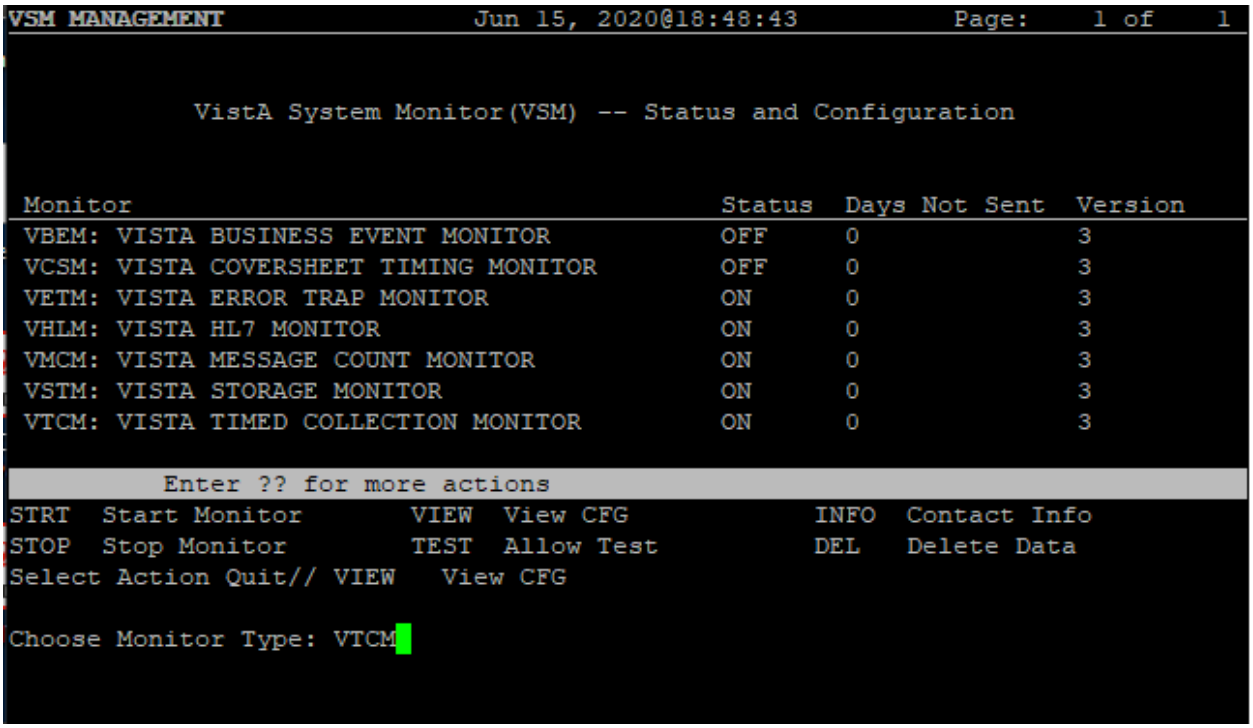
Figure 1: VSM Management—Main



NOTE: the **VSM MANAGEMENT** option requires the KMPVROPS security key.

2. Once in the "**VSM MANAGEMENT**" screen:
   a. Choose **VIEW**.
   b. Choose the monitor (e.g., **VTCM**), as shown in Figure 2:

Figure 2: VSM Management—Menu: View Action



3. The monitor chosen is then displayed, as shown in Figure 3:

Figure 3: VSM Management—View Configuration

REDACTED

NOTE: The monitor is turned on by default for production systems. If it is a test system, the monitor will be off after installation, since the **ALLOW TEST SYSTEM** default value is **NO**.

4.10 System Configuration

There are no special system configuration requirements with the VSM 3.0 software installation.

4.11 Database Tuning

There are no special database tuning requirements for the VSM 3.0 software installation.

5 Back-Out Procedure

Back-out pertains to a return to the last known good operational state of the software and appropriate platform settings.

This software provides the means to revert most functionality back to that of VSM 2.0. This is accomplished on the remote console by the CPE VSM Admins. Contact:

VA IT EPMO CPE VistA System Monitor <REDACTED@va.gov>

If this is *not* sufficient. then a patch will need to be created and deployed to all sites to revert back to full VSM 2.0 functionality.

NOTE: For patch back-out procedures, see the patch description.

5.1 Back-Out Strategy

The need for a back-out would be determined by all affected organizations. This would primarily include representatives from:

- Veterans Health Administration (VHA)
- Enterprise Program Management Office (EPMO) Capacity
- Performance Engineering (CPE)

In the case of the initial release, a back-out would include removal of data, files, and routines. In the case of future patches and releases, the back-out strategy would be dependent on the contents of the released functionality and could include restoration of file definitions, routines, or data.

5.2 Back-Out Considerations

Back-out considerations would include impact on production VistA end-users and impact on the Wide Area Network (WAN).

5.2.1 Load Testing

Not applicable for VSM.

5.2.2 User Acceptance Testing

VSM User Acceptance Testing (UAT) is performed during VistA patch testing at test sites.

5.3 Back-Out Criteria

The VSM back-out criteria follow existing VistA back-out procedures.

5.4 Back-Out Risks

The VSM back-out risks are the same risks established with existing VistA back-out procedures.

5.5 Authority for Back-Out

The authority for the need of back-out would reside with VHA and EPMO CPE representatives.

5.6 Back-Out Procedure

This software provides the means to revert most functionality back to VSM 2.0. This is accomplished on the remote console by the CPE VSM Admins. Contact:

VA IT EPMO CPE VistA System Monitor <REDACTED@va.gov>

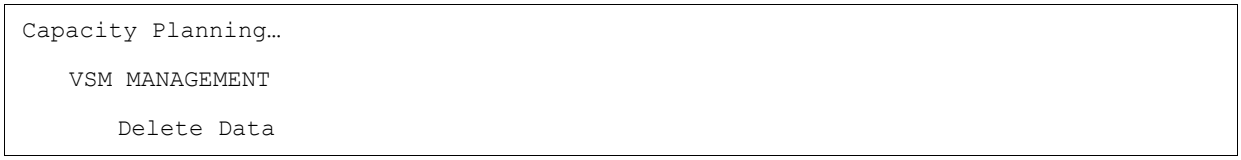
If this is *not* sufficient then a patch will need to be created and deployed to all sites that to revert to full VSM Version 2.0 functionality.

6 Rollback Procedure

Rollback pertains to data.

The VistA System Monitor (VSM) 3.0 software collects system data throughout the day and sends that data to the national database as it is collected. Data is deleted at the site upon acknowledgement from the national server that data has been received. If there is a problem with receiving the acknowledgement, then data is purged after **seven** (**7**) days. In the case that the purge does *not* work then the monitors can be stopped and all data deleted at the site using the **Delete Data** option. This option is found on the main VistA menu, as shown in Figure 4:

Figure 4: VSM Rollback Procedure—Delete Data Option



6.1 Rollback Considerations

VSM data should be deleted only if it has been determined that the automatic data management features are *not* working.

6.2 Rollback Criteria

VSM data should be deleted if there are more than **seven** (**7**) days of data in the **^KMPTMP("KMPV",** global.

6.3 Rollback Risks

The risk to rollback would be the loss of system, business and message metrics for that period of time. This risk is much less than any potential harm to a system and should be considered a low risk.

6.4 Authority for Rollback

Rollback *can* be authorized by system administrators once a problem has been identified. The Capacity and Performance Engineering (CPE) group should be informed immediately via email to the following address:

VA IT EPMO CPE VistA System Monitor <**REDACTED@va.gov**>

6.5 Rollback Procedure

Data can be deleted at the site using the **Delete Data** option. This option is found on the main VistA menu, as shown in Figure 4.

6.6 Rollback Verification Procedure

There are two ways to roll back VSM 3.0 back to VMS 2.0. The method used is dependent on the reason for the rollback:

- Can Receive HTTP Requests—If the site can successfully receive HTTP requests, the rollback mechanism can be executed from the VSM Manager Application by CPE engineers. The site will receive an HTTP message that will call VistA code to revert the configuration for each monitor back to VSM 2.0.
- *Cannot* Receive HTTP Requests—If the site *cannot* successfully receive HTTP requests, a routine is available that could be run manually to revert the configuration for each monitor back to VMS 2.0.

NOTE: VMS 2.0 software code will still exist at the site for this express purpose of facilitating a rollback if ever needed.